Predictable, efficient, and extensible Iris automation with Lithium

Michael Sammler

2.5.2022

Iris Workshop 2022

Key idea of Lithium / RefinedC

(1) Identify a subset of separation logic that can be automated using **goal-directed proof search without backtracking**

$$
\begin{array}{ll}
\text{Atom} & A ::= v \lhd_{\mathsf{v}} \tau \mid \dots \\
\text{Basic goal} & F ::= \vdash^{\Sigma}_{\text{STMT}} s \mid A_1 <: A_2 \, \{G\} \mid \dots \\
\text{Goal} & G ::= \mathsf{True} \mid F \mid H * G \mid H \mathrel{-\!\!*} G \mid G_1 \wedge G_2 \\
 & \qquad \mid \forall x.\, G(x) \mid \exists x.\, G(x) \\
\text{Left-goal} & H ::= \phi \mid A \mid H * H \mid \exists x.\, H(x) \\
\text{Contexts} & \Gamma ::= \emptyset \mid \Gamma, x \mid \Gamma, \phi \qquad \Delta ::= \emptyset \mid \Delta, A
\end{array}
$$

(2) Reduce the of verification complex programs to the Lithium fragment via **high-level abstractions**

Automating disjunction

$$P \vee Q$$

Introduction:

?

Elimination:

?

Automating disjunction

$$v \lhd_{\mathsf{v}} \phi \mathbin{@} \mathsf{optional}(\&_{\mathsf{own}}(\tau), \mathsf{null}) \triangleq \phi * v \lhd_{\mathsf{v}} \&_{\mathsf{own}}(\tau) \lor \neg\phi * v \lhd_{\mathsf{v}} \mathsf{null}$$

Introduction:

$$\textsc{S-null}\ \frac{\ulcorner \neg\phi \urcorner * G}{v \lhd_{\mathsf{v}} \mathsf{null} <: v \lhd_{\mathsf{v}} \phi \mathbin{@} \mathsf{optional}(\&_{\mathsf{own}}(\tau), \mathsf{null})\ \{G\}}$$

Elimination:

$$\textsc{O-optional-eq}\ \frac{(\ulcorner \phi \urcorner \mathrel{-\!\!*} v_1 \lhd_{\mathsf{v}} \&_{\mathsf{own}}(\tau) \mathrel{-\!\!*} G(\texttt{false}, \mathsf{False} \mathbin{@} \mathsf{bool})) \land (\ulcorner \neg\phi \urcorner \mathrel{-\!\!*} G(\texttt{true}, \mathsf{True} \mathbin{@} \mathsf{bool}))}{\vdash_{\textsc{binop}} (v_1 : \phi \mathbin{@} \mathsf{optional}(\&_{\mathsf{own}}(\tau), \mathsf{null})) = (v_2 : \mathsf{null})\ \{v, \tau.\ G(v, \tau)\}}$$

Automating invariants

$$v \lhd_{\mathsf{v}} \mathsf{atomicbool}(H_\top, H_\bot) \triangleq \exists \ell.\, v = \ell * \boxed{\exists b.\, \ell \mapsto b * (b \;?\; H_\top : H_\bot)}^{\mathcal{N}}$$

CAS-BOOL

$$\frac{\begin{array}{c}\left(v_2 \lhd_{\mathsf{v}} \&_{\mathsf{own}}(\neg b_1 \;@\; \mathsf{bool}) \mathrel{-\!\!*} G(\texttt{false}, \mathsf{False} \;@\; \mathsf{bool})\right) \wedge \\ \left((b_1 \;?\; H_\top : H_\bot) \mathrel{-\!\!*} (b_2 \;?\; H_\top : H_\bot) * \left(v_2 \lhd_{\mathsf{v}} \&_{\mathsf{own}}(b_1 \;@\; \mathsf{bool}) \mathrel{-\!\!*} G(\texttt{true}, \mathsf{True} \;@\; \mathsf{bool})\right)\right)\end{array}}{\vdash_{\mathsf{CAS}} \texttt{CAS}(v_1 : \mathsf{atomicbool}(H_\top, H_\bot), v_2 : \&_{\mathsf{own}}(b_1 \;@\; \mathsf{bool}), v_3 : b_2 \;@\; \mathsf{bool})\, \{v, \tau.\, G(v, \tau)\}}$$

Questions?

(1) **goal-directed proof search without backtracking**
(2) **guide proof via high-level abstractions**

$$
\begin{array}{lll}
\text{Atom} & A ::= v \lhd_{\mathsf{v}} \tau \mid \ldots \\
\text{Basic goal} & F ::= \vdash^{\Sigma}_{\text{STMT}} s \mid A_1 <: A_2 \, \{G\} \mid \ldots \\
\text{Goal} & G ::= \mathsf{True} \mid F \mid H * G \mid H \mathrel{-\!\!*} G \mid G_1 \wedge G_2 \\
 & \qquad \mid \forall x.\, G(x) \mid \exists x.\, G(x) \\
\text{Left-goal} & H ::= \phi \mid A \mid H * H \mid \exists x.\, H(x) \\
\text{Contexts} & \Gamma ::= \emptyset \mid \Gamma, x \mid \Gamma, \phi \qquad \Delta ::= \emptyset \mid \Delta, A
\end{array}
$$